In the Title:

Please replace the existing title with the following new title: --STORAGE MEDIUM AND METHOD AND APPARATUS FOR SEPARATELY PROTECTING DATA IN DIFFERENT AREAS OF THE STORAGE MEDIUM--.

In the Specification:

Please replace the paragraph beginning on page 2, line 5, with the following rewritten paragraph:

a1

There arise, however, several problems inherent in the prior art.

Please replace the paragraph beginning on page 2, line 7 with the following rewritten paragraph:

First, as cipher texts defined as samples or combinations of the cipher texts with unencrypted plain texts become larger in quantity, the decryption by a decipherer becomes easier. As a result, the same plain text is encrypted with the same password. Therefore, when encrypted directly with the same password, a statistic characteristic of the cipher text reflects in a statistic character of the plain text. Accordingly, a conventional method of encrypting with the same password on the storage medium presents such a problem that if a volume of the cipher texts is large enough to make a statistic process executable, the characteristics of the plain texts can be presumed easily.

Please replace the paragraph beginning on page 2, line 19 with the following rewritten paragraph:

Second, data is stored in a large capacity storage medium such as an optical disk etc. A portion of the data such as a directory portion is structured in a fixed format. A problem peculiar to the conventional method of encrypting with the same password on the storage medium is that the password is presumed by analyzing this portion, in which case other vital data are to be deciphered.

Please replace the paragraph beginning on page 2, line 26 with the following rewritten paragraph:

Third, according to the conventional method of setting the password per file, when the password of some portion is decrypted, other portions can be prevented from being decrypted. In this case, however, it is required that the different password be managed per file. This operation is troublesome and might cause a problem in which a fault such as forgetting the password and so on can easily occur.

Please replace the paragraph beginning on page 3, line 6 with the following rewritten paragraph:

Fourth, in the large capacity exchangeable storage medium such as an optical disk etc, it is possible to take the storage medium out and copy the storage medium. Therefore, the once-encrypted data is carried out and may be analyzed later on taking a

sufficient period of time. Accordingly, the problem is that the password is easy to be presumed form the cipher text.

a' cont

Please replace the paragraph beginning on page 3, line 12 with the following rewritten paragraph:

A fifth problem is that the data has hitherto been encrypted directly with the password, and hence, if the password is changed, the whole data are required to be re-encrypted.

Please replace the paragraph beginning on page 3, line 17 with the following rewritten paragraph:

a2

It is a primary object of the present invention to provide a method of and an apparatus for protecting data on a storage medium, wherein a password is not easily discovered from a cipher text.

Please replace the paragraph beginning on page 4, line 13 with the following rewritten paragraph:

a3

According to the present invention, the data is encrypted not by using the password directly as an encryption key but by using key data generated separately. The key data is encrypted with the password serving as a key, and written to the storage medium. When in the reading process, the encrypted key data is decoded with the password, thereby obtaining the key data. Then, the data is decoded with the key data.

Please replace the paragraph beginning on page 4, line 20 with the following rewritten paragraph:

Thus, the data is encrypted by use of the key data generated separately from the password, whereby the encrypted key data is, even if a cipher text is to be analyzed, merely decrypted. The password and the key data are therefore hard to analyze. This makes it feasible to prevent the password from being deciphered by analyzing the cipher text.

Please replace the paragraph beginning on page 8, line 21 with the following rewritten paragraph:

As illustrated in FIG. 4, the logical format of the storage medium (disk) 1 is shown by each sector. This sector is addressed based on a logical block address LBA. Herein, in FIG. 4, there are provided X-pieces of sectors of logical block addresses LBA being [1] through [X].

Please replace the paragraph beginning on page 8, line 26 with the following rewritten paragraph:

The region L1 for a sector starting from a head sector (LBA = 1) within the storage area of the optical disk, is allocated as a storage region for the encrypted key data PS′ [1] - PS′ [n], namely, the number of sectors in a use region of the data is n (= (X-a)), and, per section in the use region, the encrypted key data PS′ [1] - PS′ [n] are stored in the region L1.

Please replace the paragraph beginning on page 15, line 8 with the following rewritten paragraph:

a5

When in a medium logical formatting process, as in the first embodiment shown in FIG. 2, the region L1 on the optical disk 1 is stored with encrypted key data PS′ [1] - PS′ [512]. Herein, however, the encrypted data is not stored per logic sector. For example, it is assumed that a capacity of the region L1 be 4 KB. Then, supposing that the password [be] is an 8-byte/entry, as shown in FIG. 9, 512-pieces of key words (entries) PS[1] - PS [512] are generated. Subsequently, the region L1 is stored with the 512-pieces of encrypted key words PS′ [1] - PS′ [512].

Please replace the paragraph beginning on page 18, line 25 with the following rewritten paragraph:

a6

The size of the region L on the optical disk 1 can be made smaller in the third embodiment than in the first embodiment. Namely, it is required in the first embodiment that the same number of pieces of key data as the number of the logic sectors be stored. For instance, supposing that one sector is 2 KB, the storage capacity be 600 MB and the key data by 8 bytes, the region L1 is required to have a capacity of 2.4 MB. In the third embodiment, 512-pieces of key data are stored, and therefore approximately 4 KB may suffice for the region L1.